REMARKS

Claims 1-28 and 50-51 are pending in the present application. In the above amendments, claims 1, 2, 10, 14, 22 and 50 have been amended to clarify the claimed subject matter. Claims 29-49, which were previously withdrawn as being directed to a non-elected invention, are cancelled without prejudice to the filing of one or more divisional application directed thereto. New claims 53-56 have been added.

The amendments to claims 1, 2, 10, 14, 22 and 50, and the addition of new claims 53-56 are supported in the as-filed specification and drawings. For example, the amendments to claims 1, 14, 22 and 50 find support in at least paragraph [0034] of the published specification. Similarly, Applicants assert that support for new claims 53-56 is found in paragraph [0034]. Furthermore, Applicants believe that the cancellation of claims 29-49, which were previously withdrawn, results in no additional fees for the addition of new claims 53-56.

Election/Restrictions

The Office Action asserts that newly submitted claim 52 is directed to an invention that is independent or distinct from the invention originally claimed. The Office Action further asserts that since Applicants have received an action on the merits for the originally presented invention, this invention has been constructively elected by original presentation for prosecution on the merits, resulting in the withdrawal of claim 52 from consideration as being directed to a non-elected invention.

Applicants respectfully note that claim 52 is dependent from claim 1, and that claim 1 is generic of the inventions identified by the Office Action. Accordingly, Applicants respectfully request rejoinder of claim 52 upon allowance of claim 1 from which it depends.

Claim Rejections – 35 USC § 101

The Office Action rejected claims 14-21 under 35 U.S.C. §101 because the claims are alleged to be directed to non-statutory subject matter since the specification "defines the means to include software **only** [0064]." The Examiner continues to assert that merely because the specification mentions "software" in paragraph [0064] that this makes claims 14-21 non-statutory subject mater. However, this is the wrong legal standard.

Under 35 U.S.C. Section 112, Paragraph 6, an "[e]lement in a claim may be expressed as a means ... such claim shall be construed to cover corresponding structure, material, or acts described in the specification." The Examiner relies on paragraph [0064] in supporting this rejection. However, the Examiner continues to disregard even the plain language of the specification at paragraph [0064] stating that "**embodiments** may be implemented...." As Applicants have noted in prior responses, independent claims 14 and 19 are directed to "embodiments" that are **not** implemented solely by software. In particular, independent claim 14 clearly identifies the features of claim 14 as directed to "**[a] mobile user device**...," and independent claim 19 similarly identifies the features thereof as directed to "**[a] verifier apparatus**...." Applicants accordingly assert that it is clear from the language of the claims in view of the language of the specification, that the "embodiments" referred to in paragraph [0064] that are implemented by software alone do not refer to the embodiments being claimed by claims 14-21.

Applicants assert that it is not possible to have a device of claim 14 or an apparatus of claim 19 comprising software alone, without structure, and the Examiner has not provided any justification for such an interpretation. For example, the Examiner fails to explain how "**means for wirelessly outputting**," or "**means for wirelessly receiving**" can be carried out by software alone. Indeed, Applicants submit that "means for wirelessly outputting" and "means for wirelessly receiving" cannot be performed purely with software, but require hardware. Therefore, Applicants respectfully assert that it is clear that claims 14-21 are directed to hardware and any interpretation under 35 U.S.C. Section 112, Paragraph 6 should be limited to hardware. To ignore the plain language of the claims (in favor of contrary language in the specification) is inconsistent with, and lacks foundation in, the law.

In addition, Applicants note that the Office Action disregards the additional language of paragraph [0064], which states that "[w]hen implemented in software..., program code or code segment to perform the necessary tasks may be stored in a machine readable medium such as storage medium 114 and/or storage medium 124 respectively, or in a separate storage medium(s) not shown." Paragraph [0064] further states that "[p]rocessor 112 and/or 126 may perform the desired tasks." Thus, even paragraph [0064] describes that specific hardware is necessary for a device employing such software.

Accordingly, Applicants respectfully request that the Examiner withdraw the rejection of claims 14-21 under 35 U.S.C. §101.

Claim Rejections – 35 USC § 103

The Office Action rejected claims 1-3, 5-24, 26-28, 50 and 51 under 35 U.S.C. §103(a) as being allegedly obvious over U.S. Patent No. 5,761,306 (hereinafter "Lewis") in view of U.S. Patent No. 6,009,177 (hereinafter "Sudia").

These rejections are respectfully traversed in their entirety.

The Office has the burden under 35 U.S.C. § 103 to establish a prima facie case of obviousness. *In re Piasecki*, 745 F.2d 1468, 1471-72, 223 USPQ 785, 787 (Fed. Cir. 1984). To establish a prima facie case of obviousness, four basic criteria must be met. Obviousness is a question of law based on underlying factual inquiries, which inquiries include: (A) determining the scope and content of the prior art; (B) ascertaining the differences between the claimed invention and the prior art; (C) resolving the level of ordinary skill in the pertinent art; and, if applicable, and (D) secondary considerations. *Graham v. John Deere Co.*, 383 U.S. 1 (1966). Any differences between the prior art and the claims at issue must be such that they would have been obvious to a person having ordinary skill in the art at the time the invention was made. *KSR Int'l Co. v. Teleflex Inc.*, 127 S. Ct. 1727, 1734, 167 L.Ed.2d 705, 75 USLW 4289, 82 U.S.P.Q.2d 1385 (2007).

Applicants respectfully submit that the present claims are not obvious in view of the cited references under a *Graham* analysis. More specifically, the combination of Lewis with Sudia fails to teach or suggest all of the limitations of claims 1-3, 5-24, 26-28, 50 and 51, and one of ordinary skill in the art would not arrive at the limitations of claims 1-3, 5-24, 26-28, 50 and 51 in view of the differences between the cited reference and the presented claims.

A. Scope of the Prior Art

Lewis (U.S. Patent No. 5,761, 306) discloses a method in which a key server provides an active public key and a hashed replacement public key to nodes of a network. Each time a key replacement is performed, the server 16 sends a key replacement message that includes the replacement public key 150, the hash of the next replacement public key 152, and digital

signatures for the message 154, 156 to the nodes 12. (col. 7, lines 60-67, col. 8, lines 1-2). The active public key is discarded and the replacement public key replaces the active public key. (col. 3, lines 21-32). Importantly, corresponding private keys are generated for the public keys, but such private keys are not distributed to the nodes. (See, e.g., col. 8, lines 15-34). Furthermore, the public keys are only replaced at the nodes after the server 16 sends a key replacement message to the nodes instructing to replace the public key by the key server or central public key controller, and only after the first or active public key authenticates the key replacement message. (col. 8, lines 15-34 and lines 58-64; col. 9, lines 1-7).

Sudia (U.S. Patent No. 6,009,177) discloses a cryptographic system and method with a key escrow feature for verifiably splitting users' private encryption keys into components and for sending those components to trusted agents. For example, Sudia describes an embodiment in which the device includes a chip that breaks the private key into several pieces and forms a share packet for each trustee or escrow agent designated by the user. (col. 18, lines 12-26). It appears to Applicants from the disclosure in Sudia, that the purpose of keeping the private key with the trustee or escrow agent in Sudia is to verify that the user device is a trusted device and to provide a signed certificate from the master escrow center to be used for communications between devices (see, e.g., col. 20, lines 26-35), and to allow access to the private key by law enforcement for the ability to intercept and decrypt communication to and from a particular user (see, e.g., col. 30, lines 5-19). Applicants are unable to find disclosure, nor has the Examiner identified any disclosure, in Sudia describing the output of one private key and the retention of another private key at the user device. Instead, the only existing private key for the chip is both transmitted to the plurality of different entities and retained stored on the chip for subsequent use by the user device after it is transmitted to the trustee or escrow agent. (col. 17, lines 62-63).

B. Differences Between Claimed Invention and Prior Art

Claims 1-3, 5-10, 14-18, 22-24 and 50

Claim 1, as amended herein, recites "outputting the second private key from the mobile user device while retaining the first private key in the mobile user device, wherein outputting the second private key comprises wirelessly transmitting a plurality of shares of the second private

key to a plurality of different entities once, such that the second private key can be re-created by the mobile user device to replace use of the first private key and disable the first private key when the second private key is re-created and used for authentication." The Office Action admits that Lewis fails to teach or suggest transmission of any portion of either the active private key or the replacement private key. The Office Action accordingly relies on Sudia for such teachings. However, Sudia merely teaches the transmission of the single, active private key in order to obtain various certificates and in order to enable law enforcement to decrypt communications between devices, while also retaining that active private key in the user device. There is no teaching or suggestion in Sudia of transmitting a plurality of shares of a second private key to a plurality of different entities once, such that the second private key can be re-created by the mobile user device to replace use of the first private key.

Instead, Sudia would suggest to a person of ordinary skill in the art at the time of the present invention that the active or first private key must be transmitted in order to obtain the necessary certificates enabling the first private key to work. Thus, one of ordinary skill in the art would have been motivated by Sudia to transmit the first private key for enabling the first private key to function. There is no motivation in Sudia to output the second private key while retaining the first private key, such that the second private key can be re-created by the mobile user device to replace use of the first private key and disable the first private key when the second private key is re-created and used for authentication.

Finally, there is no reasonable expectation of success in modifying the teachings of Lewis and Sudia to arrive at the limitations of claim 1, as is required to establish a prima facie case of obviousness. *See In re Merck & Co., Inc.*, 800 F.2d 1091, 1097 (Fed. Cir. 1986). According to the teachings of Sudia, the first private key would not function if it has not been transmitted to the master escrow center for registration. Therefore, one of ordinary skill in the art would not reasonably expect to be able to transmit the second private key while retaining the first private key, **and** "[use] the first private key for authentication of the mobile user device" using the teachings of Sudia.

In addition to there being no teaching or suggestion by Sudia to output the second private key while retaining the first private key in the mobile user device, Sudia also teaches that the private key is both transmitted to the plurality of different entities and retained on the chip for

subsequent use by the user device after it is transmitted to the trustee or escrow agent. Therefore, Sudia further fails to teach or suggest "**outputting** the second private key." Indeed, since the point of communicating the private key to the escrow agent(s) according to Sudia is to register the private key for use by the user device, Sudia inherently requires that the communicated private key not be output, but rather that the communicated private key be retained by the user device in order for the user device to be able to communicate with other devices. Further, Sudia expressly teaches that the chip stores the private key in addition to communicating it to the escrow agent(s).

Applicants respectfully assert that Lewis and Sudia, when combined, do not teach or suggest at least "**outputting the second private key** from the mobile user device **while retaining the first private key** in the mobile user device, wherein outputting the second private key comprises wirelessly transmitting a plurality of shares of the second private key to a plurality of different entities once, such that the second private key can be re-created by the mobile user device to replace use of the first private key and disable the first private key when the second private key is re-created and used for authentication," as recited in independent claim 1 and as similarly recited in independent claim 14, and these differences between claims 1 and 14 and the combined teachings of the cited references would not have been obvious to one of ordinary skill in the art at the time the invention was made. Applicants, therefore, respectfully request that the Examiner withdraw the 35 U.S.C. § 103(a) obviousness rejection to claims 1 and 14.

Similarly, Lewis and Sudia, when combined, do not teach or suggest at least "**keep the first private key** within the mobile user device and wirelessly **output the second private key** as a plurality of shares of the second private key to a plurality of different entities once such that the second private key can be re-created by the mobile user device to replace use of the first private key and disable the first private key when the second private key is re-created and used for authentication," as recited in independent claim 22, and these differences between claim 22 and the combined teachings of the cited references would not have been obvious to one of ordinary skill in the art at the time the invention was made. Applicants, therefore, respectfully request that the Examiner withdraw the 35 U.S.C. § 103(a) obviousness rejection to claim 22.

Finally, Lewis and Sudia, when combined, do not teach or suggest at least "a storage medium coupled to the processor, configured to **store the first private key**; and a wireless

transmitter coupled to the processor to **output the second private key** as a plurality of shares of the second private key to a plurality of different entities once such that the second private key can be re-created by the mobile user device to replace use of the first private key and disable the first private key when the second private key is re-created and used for authentication, and output the second public key to the verifier device concurrent with wirelessly outputting the first public key," as recited in independent claim 50, and these differences between claim 50 and the combined teachings of the cited references would not have been obvious to one of ordinary skill in the art at the time the invention was made. Applicants, therefore, respectfully request that the Examiner withdraw the 35 U.S.C. § 103(a) obviousness rejection to claim 50.

Furthermore, the nonobviousness of independent claims 1, 14 and 22 precludes a rejection of claims 2, 3, 5-10, 15-18, 23 and 24, which depend therefrom, because a dependent claim is obvious only if the independent claim from which it depends is obvious. *See In re Fine*, 5 U.S.P.Q.2d 1596, 1600 (Fed. Cir. 1988), *see also* MPEP § 2143.03. Therefore, Applicants request that the Examiner withdraw the 35 U.S.C. § 103(a) obviousness rejection to claims 2, 3, 5-10, 15-18, 23 and 24, in addition to the rejection to independent claims 1, 14, 22 and 50.

Regarding dependent claim 10, Applicants additionally assert that the cited prior art references, when combined, at least fail to teach or suggest "preventing retransmission of the second private key," as recited in dependent claim 10. In particular, the portion identified by the Office Action in Sudia merely teaches limiting the number of times the device can be rekeyed, but does not teach or suggest preventing retransmission of a private key. Therefore, Applicants respectfully assert that dependent claim 10 would not have been obvious to a person of ordinary skill in the art at the time the invention was made considering Lewis in view of Sudia, and request that the Examiner withdraw the rejection of dependent claim 10 under 35 U.S.C. § 103(a) for this additional reason.

Claims 11-13, 19-21, 26-28 and 51

Claim 11 recites, in part, "using the second public key for authentication of the mobile user device if the first public key fails." The Office Action relies on Lewis as teaching such limitations and cites specifically to col. 8, lines 58-64 of Lewis. However, Lewis teaches the exact opposite from claim 11. Lewis teaches that in order to use the second public key, the first

public key must authenticate the key replacement message. Lewis states, "the digitial signature [Apr] is verified using Apu. If the digital signature does not match the message and the active public key (Apu), then the key replacement message is ignored (S5)." Thus, Lewis fails to teach or suggest "using the second public key for authentication of the mobile user device if the first public key fails," as recited in claims 11 and 19 and as similarly recited in claims 26 and 51. Instead, Lewis specifically states that the second public key is **not** used if the first public key fails. Furthermore, Applicants assert that Sudia fails to remedy these deficiencies of Lewis with respect to claims 11, 19, 26 and 51.

Applicants respectfully assert that Lewis and Sudia, when combined, do not teach or suggest at least "using the second public key for authentication of the mobile user device **if the first public key fails**," as recited in independent claims 11 and 19, and as similarly recited in independent claims 26 and 51, and these differences between claims 11, 19, 26 and 51 and the combined teachings of the cited references would not have been obvious to one of ordinary skill in the art at the time the invention was made. Applicants, therefore, respectfully request that the Examiner withdraw the 35 U.S.C. § 103(a) obviousness rejection to claims 11, 19, 26 and 51.

Furthermore, the nonobviousness of independent claims 11, 19 and 26 precludes a rejection of claims 12, 13, 20, 21, 27 and 28, which depend therefrom, because a dependent claim is obvious only if the independent claim from which it depends is obvious. *See In re Fine*, 5 U.S.P.Q.2d 1596, 1600 (Fed. Cir. 1988), *see also* MPEP § 2143.03. Therefore, Applicants request that the Examiner withdraw the 35 U.S.C. § 103(a) obviousness rejection to claims 12, 13, 20, 21, 27 and 28, in addition to the rejection to independent claims 11, 19, 26 and 51.

Should any of the above rejections be maintained, Applicant respectfully requests that the noted limitations be identified in the cited references with sufficient specificity to allow Applicant to evaluate the merits of such rejections. In particular, rather than generally citing whole sections or columns, Applicant requests that the each claimed element be specifically identified in the prior art to permit evaluating the references.

CONCLUSION

In light of the amendments contained herein, Applicant submits that the application is in condition for allowance, for which early action is requested.

Please charge any extension fees or overpayments that may be due with this response to Deposit Account No. 17-0026. Applicant requests **a one month** extension of time.

Respectfully submitted,

Dated: January 8, 2010

By: _____

Won Tae C. Kim, Reg. # 40,457
(858) 651 6295

QUALCOMM Incorporated
5775 Morehouse Drive
San Diego, California 92121
Telephone: (858) 658-5787
Facsimile: (858) 658-2502